Geopriv
Internet-Draft
Intended status: Standards Track
Expires: February 27, 2010

J. Winterbottom
M. Thomson
Andrew Corporation
H. Tschofenig
Nokia Siemens Networks
R. Barnes
BBN Technologies
August 26, 2009

**Use of Device Identity in HTTP-Enabled Location Delivery (HELD)**
**draft-winterbottom-geopriv-held-identity-extensions-10**

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on February 27, 2010.

Abstract

When a Location Information Server receives a request for location information (using the locationRequest message), described in the base HTTP Enabled Location Delivery (HELD) specification, it uses the source IP address of arriving message as a pointer to the location determination process. This is sufficient in environments where the location of a Device can be determined based on its IP address.

Two additional use cases are addresses by this document. In the first, location configuration requires additional or alternative identifiers from the source IP address provided in the request. In the second, an entity other than the Device requests the location of the Device.

This document extends the HELD protocol to allow the location request message to carry Device identifiers. Privacy and security considerations describe the conditions where requests containing identifiers are permitted.

Table of Contents

## 1. Introduction

Protocols for requesting and providing location information require a way for the requestor to specify the location that should be returned. In a location configuration protocol (LCP), the location being requested is the requestor's location. This fact can make the problem of identifying the Device simpler for LCPs, since IP datagrams that carry the request already carry an identifier for the Device, namely the source IP address of an incoming request. Existing LCPs, such as HELD [I-D.ietf-geopriv-http-location-delivery] and DHCP ([RFC3825], [RFC4776]) rely on the source IP address or other information present in protocol datagrams to identify a Device.

Aside from the datagrams that form a request, a location information server (LIS) does not necessarily have access to information that could further identify the Device. In some circumstances, as shown in [I-D.ietf-geopriv-l7-lcp-ps], additional identification information can be included in a request to identify a Device.

This document extends the HELD protocol to support the inclusion of additional identifiers for the Device in HELD location requests. An XML schema is defined that provides a structure for including these identifiers in HELD requests.

An important characteristic of this addition to the HELD protocol is that it also expands the potential scope of HELD beyond that of an LCP. The scope of an LCP is limited to the interaction between a Device and a LIS. That is, an LCP is limited to the Device retrieving information about their own location. With this addition, authorized third party location recipients (LRs) are able to make requests that include identifiers to retrieve location information about a particular Device.

The usage of HELD for purposes beyond the Device-LIS interaction obviously introduces a new set of privacy concerns. In an LCP, the requester is implicitly authorized to access the requested location information, because it is their own location. In contrast, a third party LR must be explicitly authorized when requesting the location of a Device. Establishing appropriate authorization and other related privacy concerns are discussed in Section 5.

### 1.1. Applications

The use of additional identifiers in HELD falls into two categories. A Device can use these parameters to provide additional identification information to a LIS. Identification information, such as the MAC address of the interface card of a Target, can be used to reduce the time required to determine the location by a LIS.

In other cases, a LIS might require Device identification before any location information can be generated.

A third party LR can be granted authorization to make requests for a given Device. In particular, network services can be permitted to retrieve location for a Device that is unable to acquire location information for itself (see Section 6.3 of [I-D.ietf-ecrit-phonebcp]). This allows use of location-dependent applications - particularly essential services like emergency calling - where Devices do not support a location configuration protocol (LCP) or they are unable to successfully retrieve location information.

## 2. Terminology

This document uses the term Location Information Server (LIS) and location configuration protocol (LCP) as described in [I-D.ietf-geopriv-l7-lcp-ps].

The term Device is used specifically as the subject of an LCP, consistent with [I-D.ietf-geopriv-http-location-delivery]. This document also uses the term Target to refer to any entity that might be a subject of the same location information. Target is used in a more general sense, including the Device, but also any nearby entity, such as the user of a Device. A Target has a stake in setting authorization policy on the use of location information. Both Device and Target are defined in [RFC3693].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 3. Device Identity

Identifiers are used as the starting point in location determination. They should not be confused with measurement information ([I-D.thomson-geopriv-held-measurements]). Measurement information is information about a Device and the time varying details of its network attachment. Identifiers might be associated with a different Device over time, but the their purpose is to identify the Device, not to describe its environment or network attachment.

### 3.1. Identifier Suitability

Use of any identifier MUST only be allowed if it identifies a single Device at a particular time. In some circumstances, certain of these identifiers are either temporary or could potentially identify multiple devices. Identifiers that are transient or ambiguous could be exploited by an attacker to either gain information about another device or to coerce the LIS into producing misleading information.

The identifiers described in this section MUST only be used where that identifier is used as the basis for location determination. Considerations relating to the use of identifiers for a Device requesting its own location are discussed in Section 5 of [I-D.ietf-geopriv-l7-lcp-ps]; this section discusses use of identifiers for authorized third party requests.

> It is tempting for a LIS implementation to allow alternative identifiers for convenience or some other perceived benefit. However, care needs to be taken to ensure that the binding between the indicated identifier and the identifier that is used for location determination is unique and not subject to attacks.

Identifiers can have a different meaning to different entities on a network. An identifier in one network context might have a completely different meaning in a different context. Errors in perspective arise in both topology (all network entities have a subjective view of the network) and time (the network changes over time).

#### 3.1.1. Subjective Network Views

Subjective views of the network mean that the identifier a requests uses to refer to one physical entity could actually apply to a different physical entity when used in a different network context. Unless an authorized third party requester and LIS operate in the same network context, each could have a different subjective view of the meaning of the identifier.

In this case, the third party receives information that is correct only within the network context of the LIS. The location information provided by the LIS is probably misleading: the requester believes that the information relates to a different entity than it was generated for.

> In IP networks, network address translation (NAT) and other forms of address modification create network contexts. Entities on either side of the point where modification occurs have a different view of the network. Private use addresses [RFC1918] are the most easily recognizable identifiers that have limited scope.

A LIS can be configured to recognize scenarios where the subjective view of a requester might not coincide with the view of the LIS. The LIS can either provide location information that takes the view of the requester into account, or it can reject the request.

> For instance, a LIS might operate within a network that uses a private address space, with NAT between that network and other networks. A third party request that originates in an external network with an IP address from the private address space might not be valid - it could be identifying an entity within another address space. The LIS can be configured to reject such requests, unless it knows by other means that the request is valid.
>
> In the same example, the requester might include an address from the external space in an attempt to identify a host within the network. The LIS could use knowledge about how the external address is mapped to a private address, if that mapping is fixed, to determine an appropriate response.

The residential gateway scenario in Section 3.1 of [I-D.ietf-geopriv-l7-lcp-ps] is a particular example of where a subjective view is permitted. The LIS knowingly provides Devices on the remote side of the residential gateway with location information, in spite of the ambiguity. The LIS provides location information with appropriate uncertainty to allow for the fact that the residential gateway serves a small geographical area.

### 3.1.2. Transient Identifiers

Some identifiers are temporary and can, over the course of time, be assigned to different physical entities. An identifier that is reassigned between the time that a request is formulated by a requester and when the request is received by the LIS causes the LIS to locate a different entity than the requester intended. The response from the LIS might be accurate, but the request incorrectly

associates this information with the wrong subject.

A LIS should be configured with information about any potentially temporary identifiers. It can use this information to identify when changes have occurred. A LIS must not provide location information if the identifier it uses might refer to a different Device. If an identifier might have been reassigned recently, or it is likely to be reassigned, it is not suitable as an identifier.

It's possible that some degree of uncertainty could persist where identifiers are reassigned frequently; the extent to which errors arising from using transient identifiers are tolerated is a matter for local policy.

## 3.2. Identifier Format and Protocol Details

XML elements are used to express the Device identity. The "target" element is used as a general container for identity information. This document defines a basic set of identifiers. An example HELD request, shown in Figure 1, includes an IP version 4 address.

```
<locationRequest xmlns="urn:ietf:params:xml:ns:geopriv:held"
                 responseTime="8">
  <locationType exact="true">geodetic</locationType>
  <device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
    <ip v="4">192.0.2.5</ip>
  </device>
</locationRequest>
```

Figure 1

A LIS that supports this specification echoes the "target" element in a successful HELD response, including the identifiers that were used as the basis for location determination. Absence of this indication means that the location information was generated using the source IP address in the request.

If an identifier is invalid, not supported by the LIS, or the requester is not authorized to use that identifier, a HELD error response of "badIdentifier". This code is registered in Section 7.3.

If the LIS requires an identifier that is not provided in the request, the desired identifiers MAY be identified in the HELD error response, using the "requiredIdentifiers" element. This element contains a list of XML qualified names [W3C.REC-xml-names11-20060816] that identify the identifier elements required by the LIS. Namespace prefix bindings for the qualified names are taken from document context. Figure 2 shows an example error indicating that the

requester needs to include a MAC address (Section 3.3.2) if the request is to succeed.

```
<error xmlns="urn:ietf:params:xml:ns:geopriv:held"
       code="badIdentifier">
  <message xml:lang="en">MAC address required</message>
  <requiredIdentifiers
      xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
    mac
  </requiredIdentifiers>
</error>
```

Figure 2

## 3.3. Identifiers

A limited selection of identifiers are included in this document. The basic Device identity schema allows for the inclusion of elements from any namespace, therefore additional elements can be defined using different XML namespaces.

### 3.3.1. IP Address

The "ip" element can express a Device identity as an IP address. An optional "v" attribute identifies the IP version. The element uses the textual format specific to the indicated IP version.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <ip v="6">2001:DB8::1:ea7:fee1:d1e</ip>
</device>
```

In situations where location configuration does not require additional identifiers, using IP address as an identifier enables authorized third party requests.

### 3.3.2. MAC Address

The media access control (MAC) address used by the IEEE 802 family of access technologies is an identifier that is assigned to a particular network device. A MAC address is a unique sequence that is either assigned at the time of manufacture of a device, or assigned by a local administrator. A MAC address rarely changes; therefore, a MAC address is an appropriate identifier for a Device.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <mac>A0-12-34-56-78-90</mac>
</device>
```

A LIS that operates on the same layer 2 segment as a Device sees the MAC address of the Device and can authenticate the device in that fashion. If a router is interposed between LIS and Device, other means of authentication are required.

### 3.3.3. TCP or UDP Port Number

On its own, a TCP or UDP port number is insufficient to uniquely identify a single host, but in combination with an IP address, it can be used in some environments to uniquely identify a Device.

Use of a particular port number can be transient; often significantly more than use of any given IP address. However, widespread use of network address translation (NAT) means that some Devices cannot be uniquely identified by IP address alone. An individual Device might be identified by a flow of packets that it generates. Providing that a LIS has sufficient knowledge of the mappings used by the NAT, an individual target on the remote side of the NAT might be able to be identified uniquely.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <ip v="6">2001:DB8::1:ea7:fee1:d1e</ip>
  <udpport>51393</udpport>
</device>
```

Use of port numbers is especially reliant on the value remaining consistent over time.

### 3.3.4. Network Access Identifier

A Network Access Identifier (NAI) [RFC4282] is an identifier used in network authentication in a range of networks. The identifier establishes a user identity within a particular domain. Often, network services use an NAI in relation to location records, tying network access to user authentication and authorization.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <nai>user@example.net</nai>
</device>
```

The formal grammar for NAI [RFC4282] permits invalid Unicode, which cannot be expressed using XML. Therefore, this expression of NAI permits escaping. Non-unicode characters (and any other character) are expressed using a backslash ('\') followed by two hexadecimal digits representing the value of a single octet.

The canonical representation of an NAI is the sequence of octets that is produced from the concatenation of UTF-8 encoded sequences of

unescaped characters and octets derived from escaped components. This sequence MUST conform to the constraints in [RFC4282].

### 3.3.5. URI

A Device can be identified by a URI. Any URI can be used providing that the requester and LIS have a common understanding of the semantics implied by use of the URI.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <uri>sip:user@example.net;gr=kjh29x97us97d</uri>
</device>
```

### 3.3.6. Hostname

A domain name can be used as the basis for identification using the "hostname" element.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <hostname>host.example.net</hostname>
</device>
```

### 3.3.7. Directory Number

Telephony devices are typically identified by the number that is used to reach them. Within enterprises, where globally accessible telephone numbers might not be used, a directory number is the usual form of identification.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <dn>7515</dn>
</device>
```

### 3.3.8. Cellular Telephony Identifiers

A range of different forms of mobile station identifiers are used for different cellular telephony systems. Elements are defined for these identifiers. The following identifiers are defined:

msisdn: The Mobile Subscriber Integrated Services Digital Network Number (MSISDN) is an E.164 number between 6 and 15 digits long.

imsi: The International Mobile Subscriber Identity (IMSI) an identifier associated with all GSM and UMTS mobile subscribers.

imei: The International Mobile Equipment Identifier (IMEI) is a unique device serial number up to 15 digits long.

min: The Mobile Identification Number (MIN) is a unique number assigned to CDMA handsets.

mdn: The Mobile Directory Number (MDN) is an E.164 number, with usage similar to MSISDN.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <msisdn>11235550123</msisdn>
</device>
```

### 3.3.9. DHCP Unique Identifier

The Dynamic Host Configuration Protocol (DHCP) uses a binary identifier for its clients. The DHCP Unique Identifier (DUID) is expressed in Option 61 of DHCPv4 (see [RFC4361]) or Option 1 of DHCPv6 and follows the format defined in Section 9 of [RFC3315]. The "duid" element includes the binary value of the DUID expressed in hexadecimal.

```
<device xmlns="urn:ietf:params:xml:ns:geopriv:held:id">
  <duid>1234567890AaBbCcDdEeFf</duid>
</device>
```

## 4. XML Schema

```
<?xml version="1.0"?>
<xs:schema
    targetNamespace="urn:ietf:params:xml:ns:geopriv:held:id"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:id="urn:ietf:params:xml:ns:geopriv:held:id"
    elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- Device Identity -->
  <xs:element name="device" type="id:deviceIdentity"/>
  <xs:complexType name="deviceIdentity">
    <xs:sequence>
      <xs:any namespace="##any" processContents="lax"
              minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:element name="requiredIdentifiers" type="id:qnameList"/>
  <xs:simpleType name="qnameList">
    <xs:list itemType="xs:QName"/>
  </xs:simpleType>

  <xs:element name="ip" type="id:ipAddress"/>
  <xs:complexType name="ipAddress">
    <xs:simpleContent>
      <xs:extension base="xs:token">
        <xs:attribute name="v" use="optional">
          <xs:simpleType>
            <xs:restriction base="xs:token">
              <xs:pattern value="[\da-fA-F]"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:attribute>
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>

  <xs:element name="mac" type="id:macAddress"/>
  <xs:simpleType name="macAddress">
    <xs:restriction base="xs:token">
      <xs:pattern value="[\da-fA-F]{2}(-[\da-fA-F]{2}){5}"/>
    </xs:restriction>
  </xs:simpleType>

  <xs:element name="udpport" type="id:portNumber"/>
  <xs:element name="tcpport" type="id:portNumber"/>
  <xs:simpleType name="portNumber">
```

```
      <xs:restriction base="xs:nonNegativeInteger">
        <xs:maxInclusive value="65535"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:element name="nai" type="xs:token"/>

    <xs:element name="uri" type="xs:anyURI"/>

    <xs:element name="dn" type="id:digits"/>
    <xs:simpleType name="digits">
      <xs:restriction base="xs:token">
        <xs:pattern value="[\d]+"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:element name="hostname" type="id:domainName"/>
    <xs:simpleType name="domainName">
      <xs:restriction base="xs:token">
        <!-- the following pattern does not include whitespace;
             whitespace is added only to conform to document
             formatting restrictions -->
        <xs:pattern value="([A-Za-z\d]([A-Za-z\d-]*[A-Za-z\d])*\.)*
                           [A-Za-z\d]([A-Za-z\d-]*[A-Za-z\d])*"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:element name="duid" type="xs:hexBinary"/>

    <xs:element name="msisdn" type="id:e164"/>
    <xs:element name="imsi" type="id:e164"/>
    <xs:element name="imei" type="id:digit15"/>
    <xs:element name="min" type="id:digit10"/>
    <xs:element name="mdn" type="id:e164"/>
    <xs:simpleType name="e164">
      <xs:restriction base="id:digit15">
        <xs:minLength value="6"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="digit15">
      <xs:restriction base="id:digits">
        <xs:maxLength value="15"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="digit10">
      <xs:restriction base="id:digits">
        <xs:length value="10"/>
      </xs:restriction>
```

```
    </xs:simpleType>

  </xs:schema>
```

## 5. Privacy Considerations

The authorization model for a location configuration protocol assumes that the LR is also the Target, and that providing that LR with information about its own location is allowed. We call this property "LCP policy". In effect, an LCP server (that is, the LIS) follows a single rule policy that states that the Target is the only authorized Location Recipient.

Note: HELD explicitly takes the position that the Target is a Device and not a person. When discussing privacy, Targets other than a Device have a stake in protecting privacy. Therefore, the more general term of Target - any potential subject of location information - is used in place of Device.

When Device identity is used, the "LCP policy" is only applicable if the LR and Target are the same entity. If they are the same, the security and privacy considerations of the base HELD protocol [I-D.ietf-geopriv-http-location-delivery] MAY be applied by a LIS. The usage of the additional identifiers defined in this document by the LR MAY cause the LIS to perform additional security verifications to take place.

LR and Target MUST be verified by the LIS to be the same identity, assuming that related identities are the same is not sufficient.

For example, it is not appropriate to apply LCP policy where a requester is authenticated by NAI and the supplied Device identity is a MAC address, even if that MAC address is currently registered with the network under the given NAI. In this case, the requester might be requesting from a different MAC address registered under the same NAI. The correct way of gaining authorization is to establish a policy that permits this particular request as a third party request.

The LCP policy does not allow requests made by third parties. If a LIS permits requests from third parties using Device identity, it assumes the rule of a Location Server (LS). As a Location Server, the LIS MUST explicitly authorize requests according to the policies that are provided by Rule Makers, including the Target. This includes authentication of requesters where required by the authorization policies.

An organization that provides a LIS that allows third party requests must provide a means for a Rule Maker to specify authorization policies as part of the LIS implementation (e.g, in the form of access control lists). Authorization must be established before allowing third party requests for the location of any Target. Until

an authorization policy is established, the LIS MUST reject requests by third parties (that is, the default policy is "deny all").

When the LIS is operated by an access network, the relationship between the Target and the LIS can be transient. However, the process of establishing network access usually results in a form of agreement between the Target and the network provider. This process offers a natural vehicle for establishing location privacy policies. Establishing authorization policy might be a manual process, an explicit part of the terms of service for the network, or an automated system that accepts formal authorization policies (see [RFC4745], [RFC4825]). This document does not mandate any particular mechanism for establishing an authorization policy.

## 6. Security Considerations

The security considerations in [I-D.ietf-geopriv-http-location-delivery] describe the use of TLS for server authentication, confidentiality and protection from modification. These protections apply to both LCP requests and the requests made by third parties.

All HELD requests containing identity MUST be authenticated by the LIS. How authentication is accomplished and what assurances are desired is a matter for policy. The base HELD protocol uses return reachability of an IP address implied by the requester being able to successfully complete a TCP handshake. It is RECOMMENDED that any means of authentication provide at least this degree of assurance. For requests that include Device identity, the LIS MUST support authentication of TLS clients.

### 6.1. Identifier Suitability

Transient and ambiguous identifiers can be exploited by malicious requests and are not suitable as a basis for identifying a Device. Section 3.1 provides further discussion on this subject.

Identifier transience of can lead to incorrect location information being provided. An attacker could exploit the use of transient identifiers. In this attack, the attacker either knows of a re-allocation of that identifier or is able to force the identifier to be re-allocated during the processing of the request.

An attacker could use this to acquire location information for another Device or to coerce the LIS to lie on its behalf if this re-allocation occurs between the time where authorization is granted and location information is granted.

Ambiguous identifiers present a similar problem. An attacker could legitimately gain authorization to use a particular identifier. Since an ambiguous identifier potentially refers to multiple Devices, if authorization is granted for one of those Devices, an attacker potentially gains access to location information for all of those Devices.

### 6.2. Location Configuration Protocol Requests

Requests made by a Device in the context of a location configuration protocol are covered by the same set of protections offered by HELD. LCP requests are authorized under an "LCP policy" that permits a Target access to location information about itself.

Identity information provided by the Device is private data that might be sensitive. The Device provides this information in the expectation that it assists the LIS in providing the Device a service. The LIS MUST NOT use identity information for any other purpose other than serving the request that includes that information.

### 6.3. Third Party Requests

Requests from third parties have the same requirements for server authentication, confidentiality and protection from modification as LCP requests. However, because the third party needs to be authorized, the requester MUST be authenticated by the LIS. In addition, third party requests MUST be explicitly authorized by a policy that is established by a Rule Maker.

More detail on the privacy implications of third party requests are covered in Section 5.

## 7. IANA Considerations

This document registers an XML namespace and schema with IANA in accordance with guidelines in [RFC3688]. It also creates a new registry for device identity types, and stipulates how new types are to be added.

### 7.1. URN Sub-Namespace Registration for urn:ietf:params:xml:ns:geopriv:held:id

This section registers a new XML namespace, "urn:ietf:params:xml:ns:geopriv:held:id", as per the guidelines in [RFC3688].

URI: urn:ietf:params:xml:ns:geopriv:held:id

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), James Winterbottom (james.winterbottom@andrew.com).

XML:

```
 BEGIN
   <?xml version="1.0"?>
   <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
   <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
     <head>
       <title>HELD Device Identity Parameters</title>
     </head>
     <body>
       <h1>Namespace for HELD Device Identity Parameters</h1>
       <h2>urn:ietf:params:xml:ns:geopriv:held:id</h2>
[[NOTE TO IANA/RFC-EDITOR: Please update RFC URL and replace XXXX
    with the RFC number for this specification.]]
       <p>See <a href="[[RFC URL]]">RFCXXXX</a>.</p>
     </body>
   </html>
 END
```

### 7.2. XML Schema Registration

This section registers an XML schema as per the guidelines in [RFC3688].

URI: urn:ietf:params:xml:schema:geopriv:held:id

Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org), James Winterbottom (james.winterbottom@andrew.com).

Schema: The XML for this schema can be found as the entirety of Section 4 of this document.

### 7.3. Registration of HELD 'badIdentifier' Error Code

This section registers the "badIdentifier" error code in the "Geopriv HELD Registries, Error codes for HELD" IANA registry.

badIdentifier This error code indicates that the Device identifiers used in the HELD request were either: not supported by the LIS, badly formatted, or that the requester was not authorized to make a erquest for that identifier.

## 8. Acknowledgements

The authors wish to thank the NENA VoIP location working group for their assistance in the definition of the schema used in this document. Special thanks go to Barbara Stark, Guy Caron, Nadine Abbott, Jerome Grenier and Martin Dawson. Bob Sherry provided input on use of URIs. Thanks to Adam Muhlbauer and Eddy Corbett for providing further corrections. Bernard Aboba provided extensive feedback on use cases and the security model; Bernard, along with Alan DeKok, also helped resolve an issue with NAIs. Ray Bellis provided motivation for the protocol port parameters.

# 9. References

## 9.1. Normative references

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, January 2004.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4361] Lemon, T. and B. Sommerfeld, "Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)", RFC 4361, February 2006.

[I-D.ietf-geopriv-http-location-delivery] Barnes, M., Winterbottom, J., Thomson, M., and B. Stark, "HTTP Enabled Location Delivery (HELD)", draft-ietf-geopriv-http-location-delivery-15 (work in progress), June 2009.

[I-D.ietf-geopriv-l7-lcp-ps] Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol; Problem Statement and Requirements", draft-ietf-geopriv-l7-lcp-ps-10 (work in progress), July 2009.

[W3C.REC-xml-names11-20060816] Hollander, D., Tobin, R., Layman, A., and T. Bray, "Namespaces in XML 1.1 (Second Edition)", World Wide Web Consortium Recommendation REC-xml-names11-20060816, August 2006, <http://www.w3.org/TR/2006/REC-xml-names11-20060816>.

## 9.2. Informative references

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC3693] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", RFC 3693, February 2004.

[RFC3825] Polk, J., Schnizlein, J., and M. Linsner, "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", RFC 3825, July 2004.

[RFC4388] Woundy, R. and K. Kinnear, "Dynamic Host Configuration Protocol (DHCP) Leasequery", RFC 4388, February 2006.

[RFC4745] Schulzrinne, H., Tschofenig, H., Morris, J., Cuellar, J., Polk, J., and J. Rosenberg, "Common Policy: A Document Format for Expressing Privacy Preferences", RFC 4745, February 2007.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

[RFC4825] Rosenberg, J., "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", RFC 4825, May 2007.

[I-D.ietf-ecrit-phonebcp] Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling", draft-ietf-ecrit-phonebcp-13 (work in progress), July 2009.

[I-D.thomson-geopriv-held-measurements] Thomson, M. and J. Winterbottom, "Using Device-provided Location-Related Measurements in Location Configuration Protocols", draft-thomson-geopriv-held-measurements-04 (work in progress), May 2009.

[LLDP] IEEE, "802.1AB, IEEE Standard for Local and Metropolitan area networks, Station and Media Access Control Connectivity Discovery", June 2005.

## Authors' Addresses

James Winterbottom
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Email: james.winterbottom@andrew.com

Martin Thomson
Andrew Corporation
Andrew Building (39)
Wollongong University Campus
Northfields Avenue
Wollongong, NSW 2522
AU

Email: martin.thomson@andrew.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

Richard Barnes
BBN Technologies
9861 Broken Land Pkwy, Suite 400
Columbia, MD 21046
USA

Phone: +1 410 290 6169
Email: rbarnes@bbn.com